(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/19661 A3

(51) International Patent Classification⁷: H04L 29/06, 12/56

(21) International Application Number: PCT/US01/41961

(22) International Filing Date: 30 August 2001 (30.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/653,045 1 September 2000 (01.09.2000) US

(71) Applicant: TOP LAYER NETWORKS, INC. [US/US]; 2400 Computer Drive, Westboro, MA 01581-1770 (US).

(72) Inventors: NARAYANASWAMY, Krishna; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). SPINNEY, Barry, A.; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). ROSS, Theodore, L.; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). PAQUETTE, Michael, D.; Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). WRIGHT, Christopher, L.; Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US).

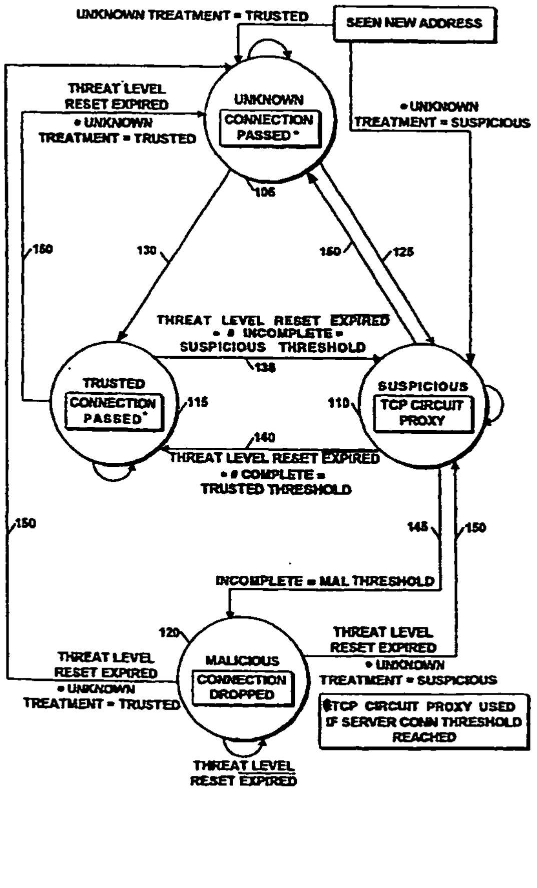
(74) Agents: CHOW, Stephen, Y. et al.;.Perkins, Smith & Cohen, LLP, One Beacon Street, Boston, MA 02108 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: SYSTEM AND PROCESS FOR DEFENDING AGAINST DENIAL OF SERVICE ATTACKS ON NETWORK NODES


UNKNOWN TREATMENT = TRUSTED
SEEN NEW ADDRESS
THREAT LEVEL RESET EXPIRED
• UNKNOWN TREATMENT = TRUSTED
UNKNOWN
CONNECTION PASSED*
• UNKNOWN TREATMENT = SUSPICIOUS
105
150
130
150
125
THREAT LEVEL RESET EXPIRED
• # INCOMPLETE = SUSPICIOUS THRESHOLD
135
TRUSTED
CONNECTION PASSED*
115
110
SUSPICIOUS
TCP CIRCUIT PROXY
140
THREAT LEVEL RESET EXPIRED
• # COMPLETE = TRUSTED THRESHOLD
150
145
150
INCOMPLETE = MAL THRESHOLD
120
THREAT LEVEL RESET EXPIRED
• UNKNOWN TREATMENT = TRUSTED
MALICIOUS
CONNECTION DROPPED
THREAT LEVEL RESET EXPIRED
• UNKNOWN TREATMENT = SUSPICIOUS
*TCP CIRCUIT PROXY USED IF SERVER CONN THRESHOLD REACHED
THREAT LEVEL RESET EXPIRED

(57) Abstract: The present invention is a network switch that maintains a relatively lightly loaded state, and at the same time protects the network servers from DOS and DDOS attacks. The switch maintains a very large table of IP addresses where it stores information such as the number of incompleted and completed connections from each address. Using this information, the switch classifies each address into a threat level: unknown, trusted, suspicious, and malicious. Each threat level is treated differently allowing the switch to provide efficient access to the server while maintaining security. Connection to the server is denied to clients classified as malicious while trusted clients are passed through to the server. Suspicious connections are proxied while unknown connection treatment may be set by the user.